BEEKDAELEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Beekdaelen

Nr. 30894

12 februari

2019

Besluit van het college van burgemeester en wethouders van de gemeente Beekdaelen houdende regels omtrent gegevensbeschermingsbeleid gemeente Beekdaelen

Hoofdstuk 1: Inleiding

1.1 Het belang van gegevensbescherming

Binnen de gemeente Beekdaelen wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat wij zorgvuldig en veilig met de persoonsgegevens omgaan. Nieuwe technologische ontwikkelingen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Wij zijn ons hier van bewust en zorgen dat de persoonlijke levenssfeer van onze burgers gewaarborgd blijft. Dit doen wij onder andere door het nemen van maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.
Het bestuur en management spelen een cruciale rol bij het waarborgen van gegevensbescherming. Wij geven middels dit beleid een duidelijke richting aan gegevensbescherming en laten zien dat wij de persoonlijke levenssfeer van burgers, medewerkers en (keten)partners waarborgen en beschermen.

1.2 Relevante wetten en verdragen

De volgende wetten en verdragen geven kaders op het gebied van gegevensbescherming:

- het Handvest van de grondrechten van de Europese Unie (EHRM);
- het Europees Verdrag voor de Rechten van de Mens (EVRM);
- het Internationaal Kinderrechtenverdrag (IVRK);
- de Nederlandse Grondwet.

Daarnaast is per 25 mei 2018 de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden. Deze verordening heeft deels nieuwe en strengere regels op het gebied van gegevensbescherming. Samen met de Uitvoeringswet AVG heeft de AVG de Wet bescherming persoonsgegevens (Wbp) vervangen.
Ons beleid voldoet aan deze internationale en nationale wettelijke kaders en verdragsregels.

1.3 Ambitie op het gebied van gegevensbescherming

Wij hebben de ambitie, maar ook de wettelijke verplichting om zoveel mogelijk te voldoen aan de kwaliteitseisen voor gegevensbescherming uit de AVG. Wij vinden dat burgers, medewerkers en (keten)partners moeten kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Niet alleen vanwege de wettelijke verplichting en het risico op handhaving door de Autoriteit Persoonsgegevens, maar ook omdat wij veel waarde hechten aan de bescherming van de persoonlijke levenssfeer van betrokkenen.
Daarnaast ambiëren wij een actief gegevensbeschermingsbeleid, dat vooral gericht is op bewustwording, een transparante en kritische cultuur en kennisoverdracht. Bovendien willen wij onze burgers zoveel mogelijk betrekken bij het onderwerp gegevensbescherming en de bijbehorende dilemma's. Goede transparante communicatie met burgers vinden wij daarom van groot belang.

1.4 Reikwijdte van het gegevensbeschermingsbeleid

Dit gegevensbeschermingsbeleid heeft betrekking op alle taken en processen waarbij persoonsgegevens worden verwerkt en waarvoor wij verantwoordelijk zijn. Het beleid is dus eveneens van toepassing op de taken en processen die wij uitbesteden, inkopen of op een andere manier hebben geregeld. Voorbeelden daarvan zijn de taken en processen die wij opdragen aan een gemeenschappelijke regeling (GR) of wanneer wij aansluiten bij landelijke voorzieningen voor gegevensverwerking, zoals bijvoorbeeld de BAG (Basisregistraties Adressen en Gebouwen).
Het beleid heeft betrekking op de hele "data levenscyclus": van het genereren of verzamelen van persoonsgegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.
Het gegevensbeschermingsbeleid staat niet op zichzelf. Het heeft raakvlakken of vertoont overlap met andere beleidsthema's als informatiebeveiliging, integriteit, kwaliteitszorg, personeel en organisatie en communicatie.

Hoofdstuk 2: Gegevensbeschermingsbeleid

2.1 Doel van het gegevensbeschermingsbeleid

Het doel van dit beleid is het vaststellen van algemene kaders voor het zorgvuldig en verantwoord omgaan met persoonsgegevens en het respecteren van de privacy van burgers, medewerkers en (keten)partners.
Daarnaast draagt het gegevensbeschermingsbeleid bij aan:

- Het vertrouwen dat burgers, medewerkers en (keten)partners hebben in de gemeente, die hun persoonsgegevens verwerkt of laat verwerken;
- Het maatschappelijk draagvlak voor maatregelen op het gebied van gegevensbescherming;
- Een betere verantwoording aan controlerende organen of personen als de gemeenteraad, controller, accountant, de rechterlijke macht, de Functionaris Gegevensbescherming [1] en de Autoriteit Persoonsgegevens [2];
- De manier waarop wij kunnen inspelen op (Europese) wettelijke en technologische ontwikkelingen;
- Het beheersen van de risico's op imagoschade, boetes en schadevergoedingen.

2.2 Opbouw van het gegevensbeschermingsbeleid

Dit beleid stelt de algemene kaders vast waarbinnen wij de gegevensbescherming regelen. Het is een kapstokbeleid dat de basis is voor de uitwerking van alle aspecten van onze bedrijfsvoering, zowel binnen als buiten onze organisatie, voor zover daarbij sprake is van de verwerking van persoonsgegevens.
De vertaling van het gegevensbeschermingsbeleid vindt plaats in een reglement, protocollen en werkprocessen en –instructies. In **bijlage 1** is dit schematisch weergegeven.

2.3 Uitgangspunten voor gegevensbescherming

Wij gaan behoorlijk en zorgvuldig om met persoonsgegevens. Wij eerbiedigen de rechten van personen waarvan wij persoonsgegevens verwerken of laten verwerken. Wij houden ons daartoe aan de volgende strategische en operationele uitgangspunten.

A. <u>Uitgangspunten op strategisch niveau</u>

Afspraken met (keten)partners
Als wij persoonsgegevens uitwisselen met externe (keten)partners en uitvoeringsorganisaties, maken wij daarover vooraf goede schriftelijke afspraken met elkaar. Deze afspraken voldoen aan de wet. De gemeente controleert deze afspraken. Daarmee laten wij zien dat wij de bescherming van de persoonsgegevens van onze burgers, medewerkers en (keten)partners serieus nemen.
Controle
Wij laten onafhankelijk nagaan of wij ons gegevensbeschermingsbeleid naleven. Dit gebeurt zowel door de Functionaris Gegevensbescherming als door de accountant en de controller. Ook onze gemeenteraad houdt toezicht op de naleving van het beleid. Het college van burgemeester en wethouders legt namelijk aan de gemeenteraad verantwoording af over de manier waarop zij omgaat met gegevensbescherming.
Sluitend beleid (compliance)
Ons beleid is een sluitend stelsel van afspraken. Deze afspraken zorgen er samen voor dat wij aantoonbaar voldoen aan de wet- en regelgeving op het gebied van gegevensbescherming. Hiermee tonen wij aan "AVG compliant" te zijn.
Sturing
Het college van burgemeester en wethouders is eindverantwoordelijk voor het naleven van het gegevensbeschermingsbeleid. Het college stuurt op de uitvoering van het beleid, evalueert periodiek en stelt het beleid waar nodig bij.
Transparantie
Wij communiceren duidelijk en pro-actief over ons beleid op het gebied van gegevensbescherming. Dit doen wij door vooraf onze burgers, medewerkers en (keten)partners te informeren over wat wij met hun persoonsgegevens gaan doen en met welk doel. Daarnaast geven wij burgers op bepaalde werkterreinen, zoals het sociaal domein, specifieke en doelgerichte informatie.
Verantwoording afleggen (Accountability)
Ons college van burgemeester en wethouders kan op elk gewenst moment bestuurlijk verantwoording afleggen over de naleving van het gegevensbeschermingsbeleid. Datzelfde geldt voor onze gemeenteraad en onze burgemeester. Ook zij zijn in enkele gevallen namelijk verantwoordelijk voor de verwerking van persoonsgegevens.

1) Voor een gemeente is de aanstelling van een Functionaris Gegevensbescherming verplicht. De taken en de verantwoordelijkheden van de Functionaris Gegevensbescherming worden nader toegelicht in hoofdstuk 3.
2) De Autoriteit Persoonsgegevens is de nationale toezichthouder op het gebied van gegevensbescherming en privacy.

B. Uitgangspunten op operationeel niveau

Beveiliging
Wij nemen passende technische en organisatorische maatregelen om de persoonsgegevens die wij gebruiken te beveiligen.
Bewaartermijn
Wij bewaren persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor wij deze hebben verzameld. Het bewaren van persoonsgegevens kan nodig zijn om onze taken goed te kunnen uitvoeren of om wettelijke verplichtingen te kunnen naleven. Persoonsgegevens waarvan de bewaartermijn is verstreken, vernietigen wij.
Dataminimalisatie
Wij verwerken alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. Wij streven daarbij naar minimale gegevensverwerking. Waar dat mogelijk is zullen wij minder of geen persoonsgegevens verwerken.
Doelbinding
Wij verzamelen uitsluitend persoonsgegevens voor uitdrukkelijk omschreven doelen. Wij verwerken persoonsgegevens niet verder op een manier die niet past bij het doel waarvoor wij de gegevens hebben verkregen.
Grondslag
Wij gebruiken alleen persoonsgegevens als daarvoor een wettelijke grondslag is en het gebruik noodzakelijk is om onze taken te kunnen uitvoeren.
Integriteit en vertrouwelijkheid
Wij behandelen persoonsgegevens vertrouwelijk. Wij laten alleen persoonsgegevens verwerken door personen met een geheimhoudingsplicht.
Kwaliteit
Wij zorgen ervoor dat de persoonsgegevens die wij gebruiken juist, nauwkeurig en actueel zijn.
Proportionaliteit
Wij letten erop dat de inbreuk op de privacy van de persoon van wie wij persoonsgegevens verwerken of laten verwerken, evenredig is in verhouding tot het doel waarvoor de persoonsgegevens worden verwerkt.
Rechten van betrokkenen
Wij handelen verzoeken, vragen en klachten over de manier waarop wij omgaan met persoonsgegevens voortvarend en laagdrempelig af.
Rechtmatigheid
Wij verwerken persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier.
Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, verwerken wij persoonsgegevens op een voor betrokkene zo min mogelijk nadelige manier. Wij kijken eerst of er andere manieren zijn waarop wij persoonsgegevens kunnen verwerken, die de privacy van betrokkene minder schaden.

Hoofdstuk 3: Rollen en verantwoordelijkheden

Wij hebben gegevensbescherming ingebed in onze organisatie. Voor onze bestuurders en medewerkers, op ieder niveau, is duidelijk welke rollen er binnen onze gemeente zijn op het gebied van gegevensbescherming. Ook weet iedereen wie voor welk onderdeel van gegevensbescherming verantwoordelijk is en welke rol en verantwoordelijkheid hij zelf heeft. Hierna gaan wij daarop verder in.
Verwerkingsverantwoordelijke
Wij hebben voor iedere gegevensverwerking in de gemeente bepaald, wie verantwoordelijk is voor het verwerken van persoonsgegevens. Voor verreweg de meeste verwerkingen van persoonsgegevens is het college van burgemeester en wethouders verantwoordelijk. In andere gevallen is de gemeenteraad of de burgemeester echter “verwerkingsverantwoordelijke.” De verwerkingsverantwoordelijke is voor die gegevensverwerking bestuurlijk eindverantwoordelijk voor de bescherming van persoonsgegevens.
Gemeenteraad
De gemeenteraad stelt de uitgangspunten voor het gegevensbeschermingsbeleid vast. Ook controleert de gemeenteraad hoe het college van burgemeester en wethouders in onze gemeente omgaat met gegevensbescherming.
College van burgemeester en wethouders
Het college van burgemeester en wethouders stelt het gegevensbeschermingsbeleid en wijzigingen daarop vast. Daarnaast is het college bestuurlijk eindverantwoordelijk voor de manier waarop de gemeente omgaat met gegevensbescherming.
Portefeuillehouder

Het college van burgemeester en wethouders heeft uit haar midden een portefeuillehouder aangewezen en deze het taakveld gegevensbescherming toegewezen. De portefeuillehouder verdedigt zaken die betrekking hebben op gegevensbescherming in vergaderingen van onze gemeenteraad en andere overleggen. Ook vertegenwoordigt de portefeuillehouder het college van burgemeester en wethouders in contacten met bijvoorbeeld burgers.

Gemeentesecretaris/algemeen directeur

De gemeentesecretaris/algemeen directeur staat aan het hoofd van alle medewerkers in de gemeente. Deze is eindverantwoordelijk voor de manier waarop de medewerkers omgaan met gegevensbescherming. Daarnaast stuurt hij het privacyteam aan en ziet samen met de Functionaris Gegevensbescherming toe op de totstandkoming van een privacy auditplan.

De gemeentesecretaris/algemeen directeur rapporteert regelmatig aan de portefeuillehouder.

Directeuren/afdelingshoofden

De directeuren/afdelingshoofden zijn samen verantwoordelijk voor de sturing op het gegevensbeschermingsbeleid en de naleving daarvan. Het directieteam:

- Beoordeelt in samenspraak met het privacyteam regelmatig of er specifiek gegevensbeschermingsbeleid nodig is op een bepaald werkveld of aanpassingen op dat beleid nodig zijn;
- Maakt gegevensbescherming tot vast agendapunt van werkoverleggen;
- Zorgt ervoor dat de Functionaris Gegevensbescherming en het privacyteam naar behoren en op een zo vroeg mogelijk moment worden betrokken bij alle zaken waarbij gegevensbescherming een rol speelt;
- Stuurt op risico's op het gebied van gegevensbescherming.

Proceseigenaren

Iedere verwerking van persoonsgegevens waarvoor wij binnen de gemeente verantwoordelijk zijn, hebben wij toegewezen aan een proceseigenaar. Een proceseigenaar is een directeur/afdelingshoofd die moet controleren of de gegevensverwerking waarvoor hij verantwoordelijk is, wordt uitgevoerd volgens de uitgangspunten van het gegevensbeschermingsbeleid. Ook ziet hij erop toe dat ons register van verwerkingen actueel is en blijft.

Proceseigenaren rapporteren regelmatig in het privacyteam.

Privacyteam

De gemeente Beekdaelen heeft een privacyteam. Dit team vertegenwoordigt een aantal kernfuncties in de organisatie. Het bestaat uit de portefeuillehouder, de gemeentesecretaris/algemeen directeur, de proceseigenaren, de Privacy Officer, de Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO). De FG en de CISO hebben een adviserende rol. Het privacyteam kan op afroep worden uitgebreid, bijvoorbeeld met een communicatieadviseur.

Het privacyteam adviseert het college van burgemeester en wethouders over het gegevensbeschermingsbeleid en de uitvoering, evaluatie en bijstelling daarvan. Ook draagt het team bij aan het overdragen van kennis en aan cultuurverandering. Daarnaast vormt het team het aanspreekpunt voor de privacy auditoren.

Privacy officer

De Privacy Officer (PO) is samen met het privacyteam de beheerder van het gegevensbeschermingsbeleid van onze gemeente. De PO rapporteert aan het privacyteam over de voortgang en kwaliteit van de uitvoering van het gegevensbeschermingsbeleid. Hij doet aanbevelingen om dit beleid verder te optimaliseren. Hij ondersteunt de directeuren/afdelingshoofden bij het opstellen/uitwerken van specifiek beleid voor een bepaald taakveld. Hij voert samen met de medewerkers en na advies van de Functionaris Gegevensbescherming Data Protection Impact Assessements (DPIA's) uit. Ook voert hij de dagelijkse werkzaamheden uit op het gebied van gegevensbescherming. Tenslotte is hij binnen onze gemeente de vraagbaak voor zaken op het gebied van gegevensbescherming.

Medewerkers

Iedere medewerker is op zijn taakveld op het gebied van gegevensbescherming verantwoordelijk voor het naleven van de wet, het beleid van de gemeente en de uitwerking daarvan. Zo is iedere medewerker bijvoorbeeld verantwoordelijk voor het direct melden van beveiligingsincidenten of datalekken volgens de daarvoor geldende procedure.

Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) houdt onafhankelijk toezicht op de manier waarop wij omgaan met gegevensbescherming. De FG adviseert de gemeente en de (keten)partners die voor haar persoonsgegevens verwerken gevraagd en ongevraagd over hun verplichtingen. Hij controleert de toewijzing en uitvoering van rollen en verantwoordelijkheden voor gegevensbescherming in onze gemeente. Hij ziet erop toe dat wij onze medewerkers opleiden op het gebied van gegevensbescherming en bewust maken van hun verantwoordelijkheden en levert daaraan een bijdrage. De FG geeft advies over de uitvoering van een DPIA en ziet toe op de uitvoering daarvan. Hij treedt op als aanspreekpunt, zowel intern als extern.

De FG rapporteert rechtstreeks aan de gemeentesecretaris/algemeen directeur en het orgaan binnen de gemeente dat verwerkingsverantwoordelijke is (het college van burgemeester en wethouders, respectievelijk de burgemeester of de gemeenteraad).

Hoofdstuk 4: Kwaliteitsborging

De AVG bepaalt dat wij moeten kunnen aantonen dat wij voldoen aan de eisen die deze wet stelt aan gegevensbescherming. Dit heet "accountability". Met dit gegevensbeschermingsbeleid en de uitwerking daarvan heeft de gemeente Beekdaelen een sluitend stelsel van afspraken gerealiseerd dat noodzakelijk is voor de verwerking van persoonsgegevens. Om te kunnen voldoen aan de eis van "accountability" is het nodig om de kwaliteit van gegevensbescherming te optimaliseren en te borgen. Daarvoor hebben wij gegevensbescherming opgenomen in onze management- en controlcyclus (de zogenaamde "Plan Do Check Act-cyclus)". Op bestuurlijk en ambtelijk niveau, van directeur tot medewerker, moet continu aandacht zijn voor gegevensbescherming en moet dit onderwerp vast op de overlegagenda staan. Alleen wanneer wij vanuit verschillende rollen de kwaliteit van gegevensbescherming beoordelen en optimaliseren, kunnen wij aantoonbaar voldoen aan de eisen die de AVG aan gegevensbescherming stelt.
Onze management- en controlcyclus op het gebied van gegevensbescherming bestaat uit de volgende onderdelen:

- *Bewustzijnstrajecten*

Wij investeren in voortdurende bewustzijnstrajecten op het gebied van gegevensbescherming voor onze medewerkers, directeuren/afdelingshoofden en bestuurders. Deze trajecten bestaan uit een aantal delen. Aan de ene kant bestaan zij uit algemene en op het taakveld afgestemde specifieke opleidingen op het gebied van gegevensbescherming. Aan de andere kant verbeteren wij het bewustzijn op dit gebied door gegevensbescherming vast agendapunt te maken van de verschillende werkoverleggen in onze gemeente. Daarmee maken wij dilemma's op het gebied van gegevensbescherming bespreekbaar en stimuleren wij medewerkers om beveiligingsincidenten en datalekken te melden.

- *Controlverklaringen*

Wij maken gebruik van controlverklaringen. Daarin leggen de proceseigenaren jaarlijks verantwoording af of de verwerkingen van persoonsgegevens worden uitgevoerd volgens het gegevensbeschermingsbeleid. Ook geven zij aan waar sprake is van afwijkingen en welke maatregelen zij hebben genomen om de risico's voor gegevensbescherming te beheersen.

- *Privacy audits*

Wij voeren regelmatig privacy audits uit volgens een auditplan. Dit auditplan vindt plaats op basis van een goede risicoanalyse. Voor het uitvoeren van risicoanalyses maken wij gebruik maken van DPIA's.

- *Planning en control*

Wij hebben gegevensbescherming als vast onderdeel opgenomen in onze jaarstukken. Daarmee legt het college van burgemeester en wethouders verantwoording af aan de gemeenteraad over hoe zij omgaat met gegevensbescherming. Ook geeft zij de gemeenteraad daarmee inzicht in de risico's op het gebied van gegevensbescherming en de maatregelen die het college heeft genomen om deze te beheersen.

- *Rapportage Functionaris Gegevensbescherming*

De Functionaris Gegevensbescherming rapporteert jaarlijks aan het college van burgemeester en wethouders over de manier waarop wij het afgelopen jaar met gegevensbescherming zijn omgegaan. Ook doet hij in zijn rapport aanbevelingen. Omdat wij transparantie hierin belangrijk vinden, stuurt het college het rapport ter kennisgeving aan de gemeenteraad.

BEEKDAELEN

Bijlage 1: Schematisch overzicht van het gemeentelijk gegevensbeschermingsbeleid